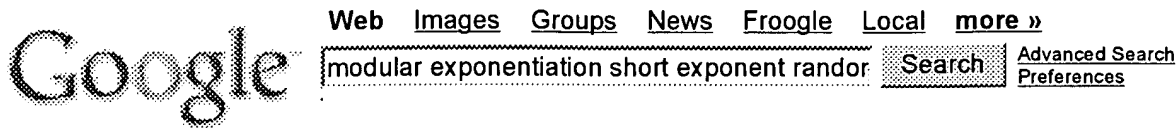


Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S26	405	708/250.ccls.	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/08/03 08:54
S25	378	708/250.ccls.	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2005/08/03 08:54
S27	3	("6285761").URPN.	USPAT	OR	OFF	2005/08/03 09:17
S28	11	patel-sarvar.in.	USPAT	OR	OFF	2005/08/03 09:38
S29	14	short\$4 adj exponent\$1	USPAT	OR	OFF	2005/08/03 10:02
S30	410	380/44.ccls.	USPAT	OR	OFF	2005/08/03 10:03
S31	194	380/44.ccls. and (modul\$2)	USPAT	OR	OFF	2005/08/03 10:04
S33	576	380/46.ccls.	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/08/03 10:16
S32	81	380/44.ccls. and (modul\$2) and prime	USPAT	OR	OFF	2005/08/03 10:16

MT H



Web Results 1 - 10 of about **43,400** for **modular exponentiation short exponent random number**. (0.26 sec)

[PDF] **Short Paper**

File Format: PDF/Adobe Acrobat - [View as HTML](#)

port the hardware or software needed for **modular exponentiation** ...
the public
exponent, as in the RSA setting. Next, he chooses a **random number**
v ...

www.iis.sinica.edu.tw/JISE/2004/200407_10.pdf - [Similar pages](#)

Sponsored Links

Random number generator

A **random number** generator, **random** selection and **random** name generator
www.supercoolbookmark.com/random/

[PDF] **Short Paper**

File Format: PDF/Adobe Acrobat - [View as HTML](#)

volves **modular exponentiation**. Since **modular exponentiation** takes a great deal
of time to ... The smart card needs to generate 2s **random numbers**, namely, b ...

www.iis.sinica.edu.tw/JISE/2000/200011_04.pdf - [Similar pages](#)

rand48(3) - pseudo random number generators and initialization ...

The rand48 family of functions generates pseudo-**random numbers** using a ...
with the **exponent** set such that the values produced lie in the interval [0.0, ...

www.gsp.com/cgi-bin/man.cgi?section=3&topic=rand48 - 13k - [Cached](#) - [Similar pages](#)

[PDF] **An Approach Towards Rebalanced RSA-CRT with Short Public Exponent**

File Format: PDF/Adobe Acrobat - [View as HTML](#)

and secret **exponent**. The first **modular exponentiation** gives the result C ...
problem is almost equivalent to "how many **random numbers** of 512 bits or 513 ...

eprint.iacr.org/2005/053.pdf - [Similar pages](#)

[PDF] **An Improved Pseudorandom Generator Based on Hardness of Factoring**

File Format: PDF/Adobe Acrobat - [View as HTML](#)

half of a fixed-base **modular exponentiation** (to be precise, our **exponent** is $n/2 - O(\log n)$... A simple unpredictable pseudo-**random number**. generator. ...

eprint.iacr.org/2002/131.pdf - [Similar pages](#)

ECECS 578 (Cheng) 1/28/99

... int, **Random**) is a constructor that generates a large **random number** that is
... The **modular exponentiation** itself can be implemented using the method ...

cheng.eecs.uc.edu/578/1-28.html - 7k - [Cached](#) - [Similar pages](#)

[PDF] **Applications of The Montgomery Exponent**

File Format: PDF/Adobe Acrobat - [View as HTML](#)

the **exponent** X is **short** (eg, **modular** squaring and RSA. verification). We also
illustrate the potential ... Alice chooses (uniformly) a **random number** ...

www.weizmann.ac.il/home/fezuk/publications/gueron_zuk_mexp_ITCC2005.pdf - [Similar pages](#)

[PDF] **On Diffie-Hellman Key Agreement with Short Exponents**

File Format: PDF/Adobe Acrobat - [View as HTML](#)

Q1: For a **random** prime p, what is the expected **number** of bits k of x leaked? ...

Thus all aspects of the **short-exponent** discrete ...

www3.sympatico.ca/wienerfamily/Michael/MichaelIPapers/dhshortexp.pdf - [Similar pages](#)

OPENCORES.ORG

MTA

1.1 To generate the primes p and q , generate a **random number** of bit length $b/2$
... 3 Choose an integer e known as the public **exponent** or encryption **exponent**, ...
www.opencores.org/articles.cgi/view/8 - 37k - Aug 2, 2005 - [Cached](#) - [Similar pages](#)

Section 10.4: Going Farther: Cryptography Using the "Lumberjack's ...

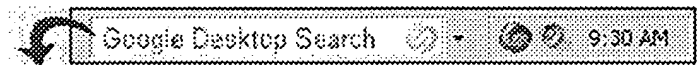
We have seen an applet before which uses the fast **modular exponentiation** ...

Alice and Bob secretly pick **random numbers**, which we will call a and b ...

www.math.mtu.edu/mathlab/COURSES/holt/dnt/primitive4.html - 22k - [Cached](#) - [Similar pages](#)

Google

Result Page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next](#)



Free! Instantly find your email, files, media and web history. [Download now.](#)

modular exponentiation short exponi [Search](#)

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2005 Google

MTA